杭州电子科技大学

网络安全理论与技术实验

实 验 报 告

学　　院	网络空间安全学院
专　　业	网络工程
班　　级	18272412
学　　号	18041618
学生姓名	廖越强
教师姓名	高梦州
完成日期	2020.12.11
成　　绩	

实验一　安全端口实验

一、　实验目的

(1)验证交换机端口安全功能配置过程。

(2)验证访问控制列表自动添加 MAC 地址的过程。

(3)验证对违规接入终端采取的各种动作的含义。

(4)验证安全端口方式下的终端接入控制过程。

二、　实验原理

由于交换机端口 1 设置为安全端口,且将访问控制列表中的最大 MAC 地址数设置为 2,因此,当分别将终端 A 和终端 B 接人交换机端口 l,且向交换机端口 1 发送 MAC 帧后,访问控制列表中已经添加终端 A 和终端 B 的 MAC 地址。当终端 C 接人交换机端口 1 且向交换机端口 1 发送 MAC 帧时,由于 MAC 帧的源 MAC 地址不属于访问控制列表中的 MAC 地址,且访问控制列表中的 MAC 地址数已经达到最大地址数 2.,因此,交换机丢弃该 MAC 帧。

三、　实验环境/实验拓扑图

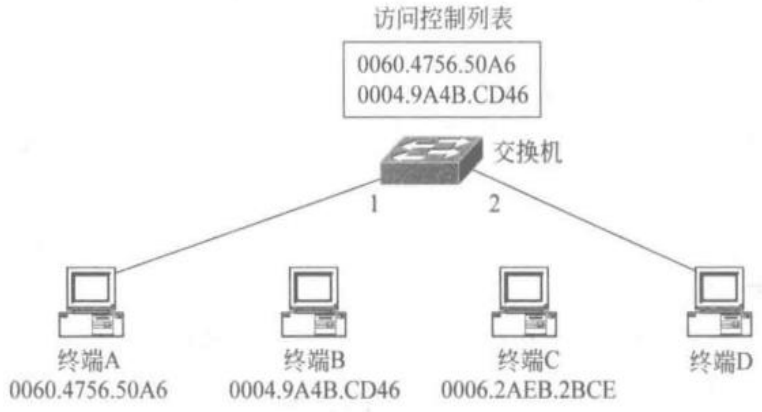
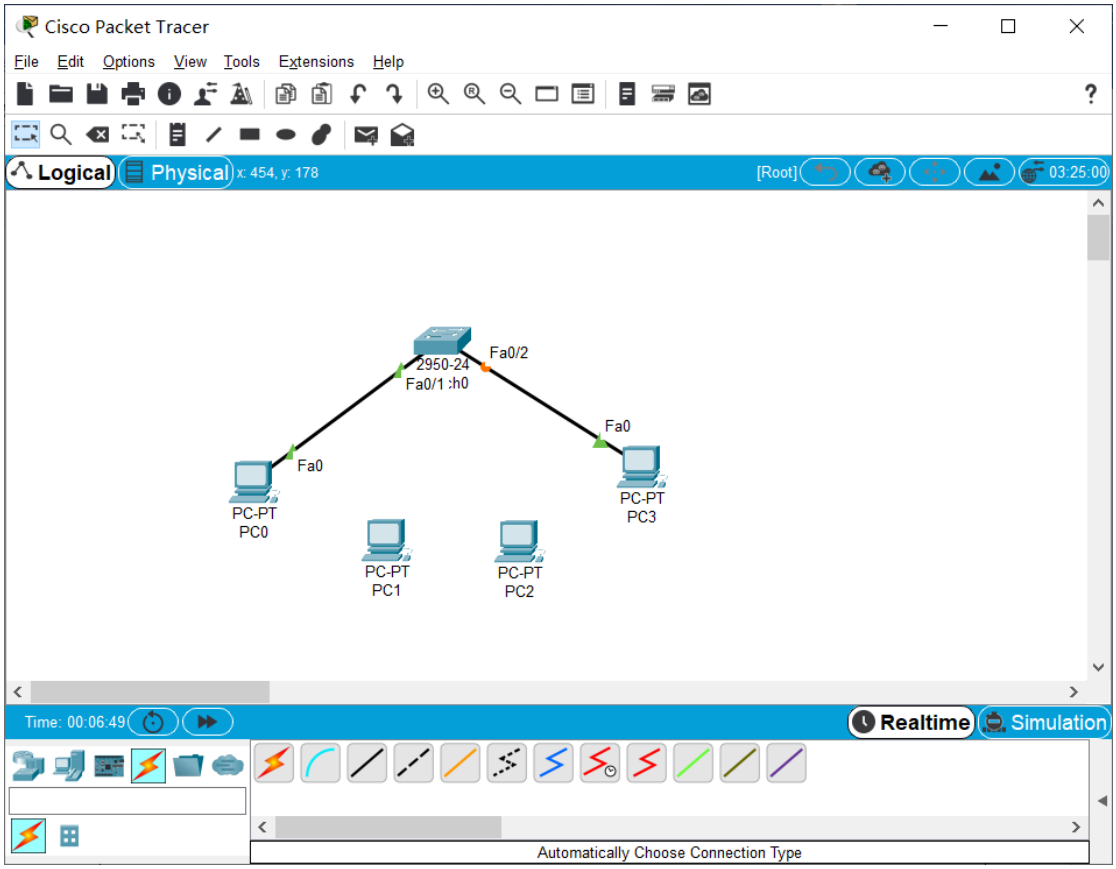


图 4.4　安全端口方式下终端接入控制过程

四、 主要操作步骤及实验结果记录

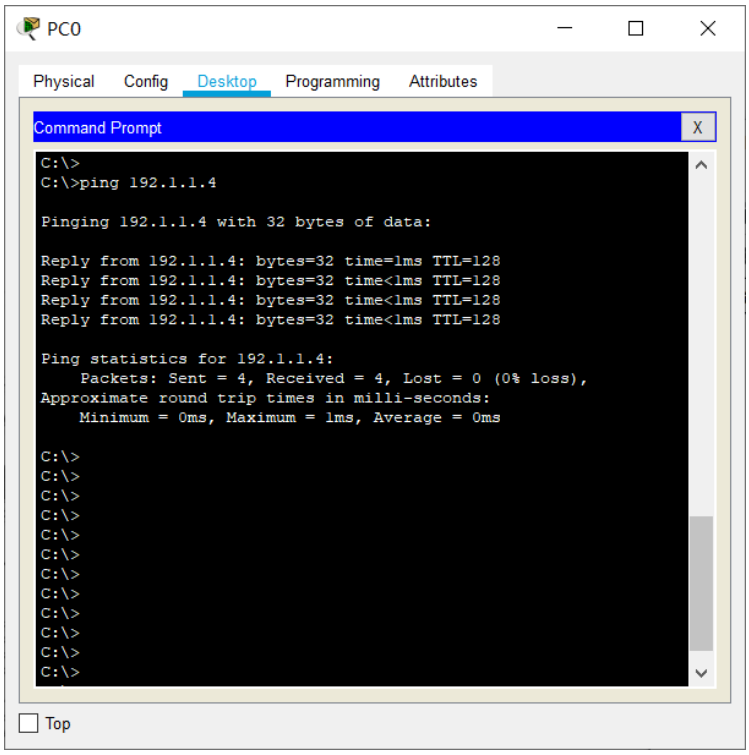
1. 完成拓扑图连接，并配置相应的网络信息



配置 fastethernet0/1 安全功能

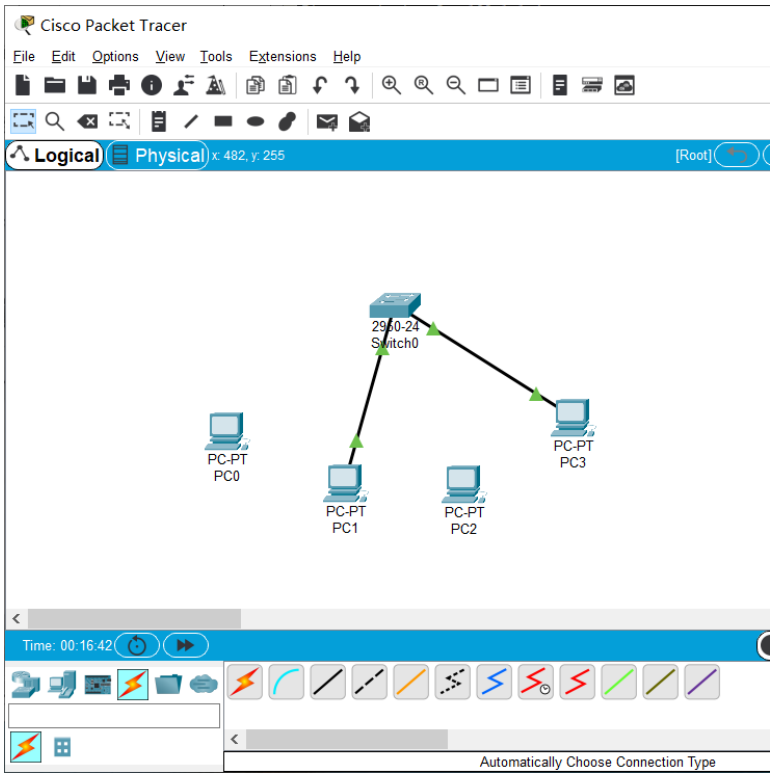
```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#
```

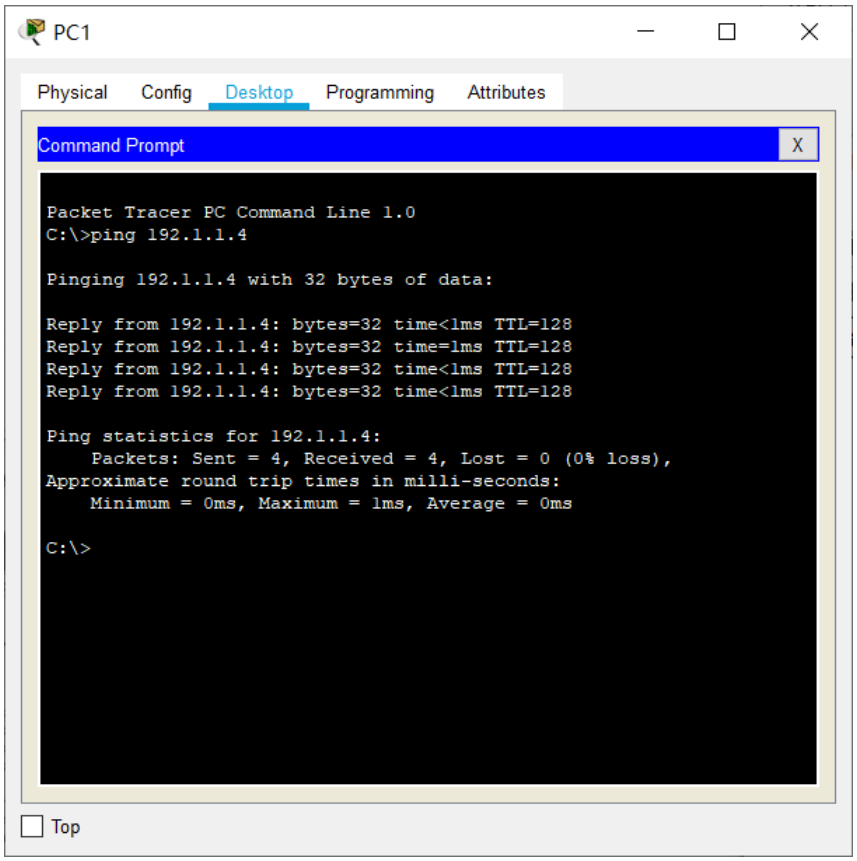
2. 使用 pc0 发送 ICMP 包给 pc3，如图，能正常发送并接受响应



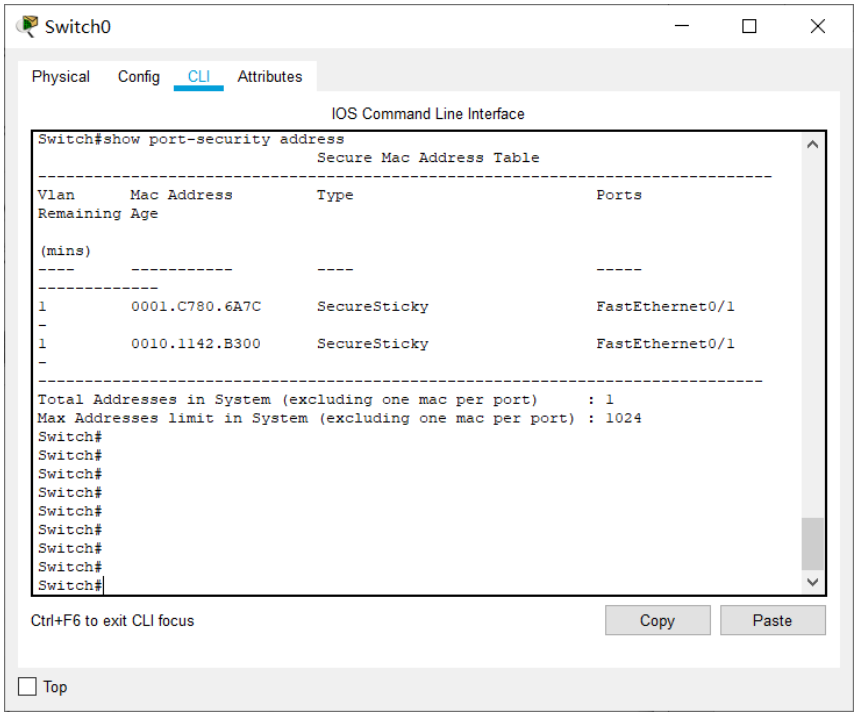
3. 删除 pc0 与交换机的连接，将 pc1 接入交换机的 fastethernet0/1 接口

使用 pc1 发送 ICMP 包给 pc3，能正常发送并响应



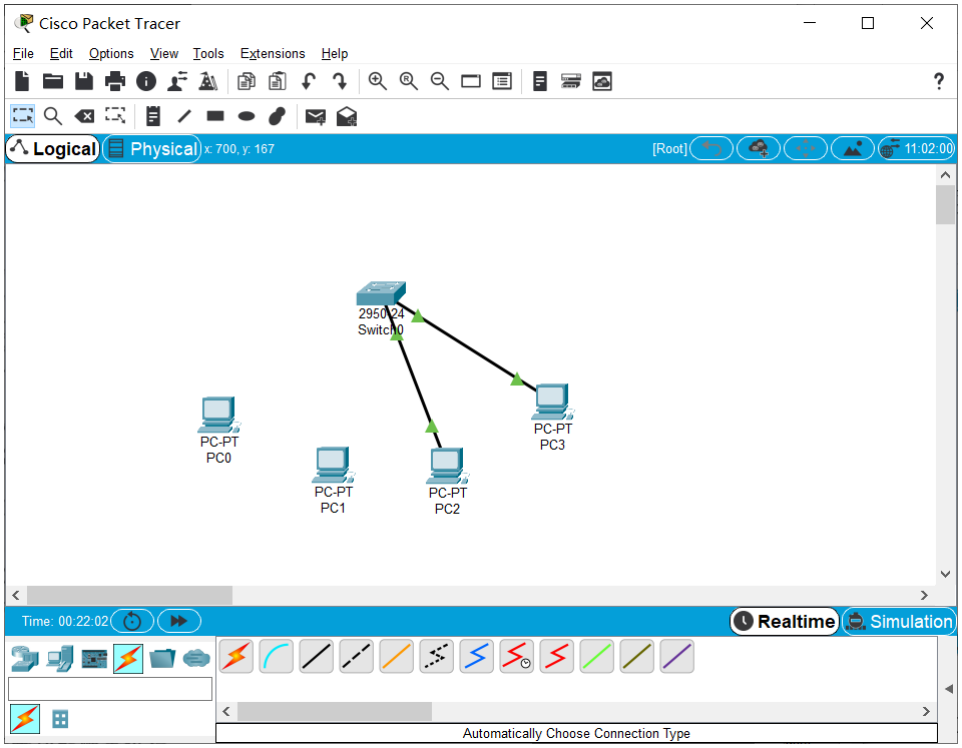


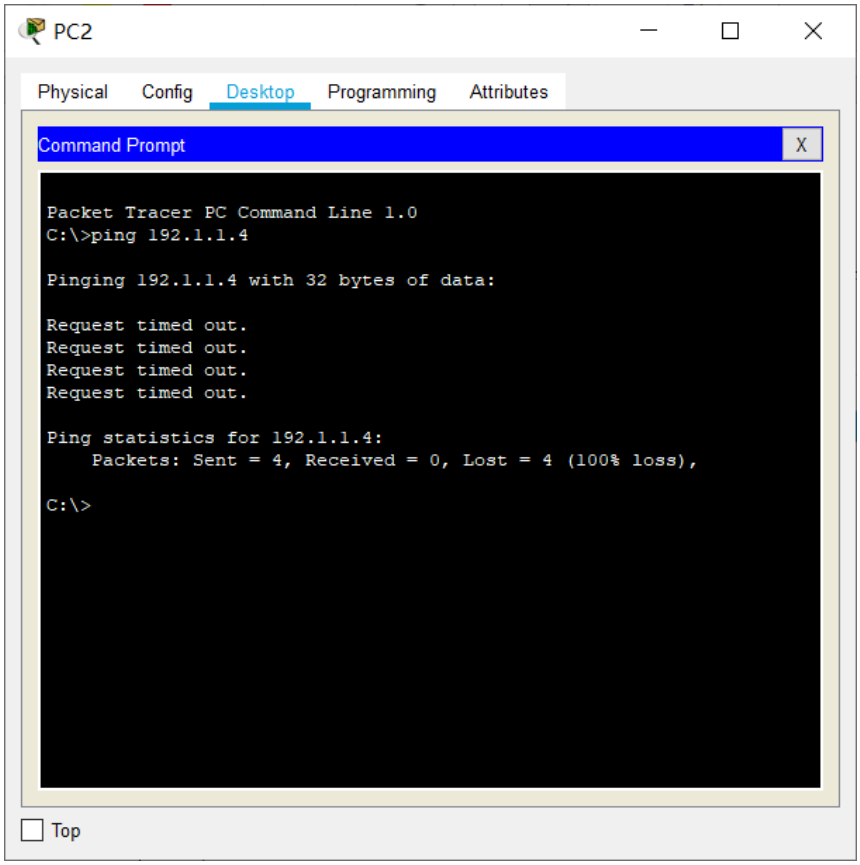
4. 查看访问控制列表中的 mac 地址（show port-security address ）



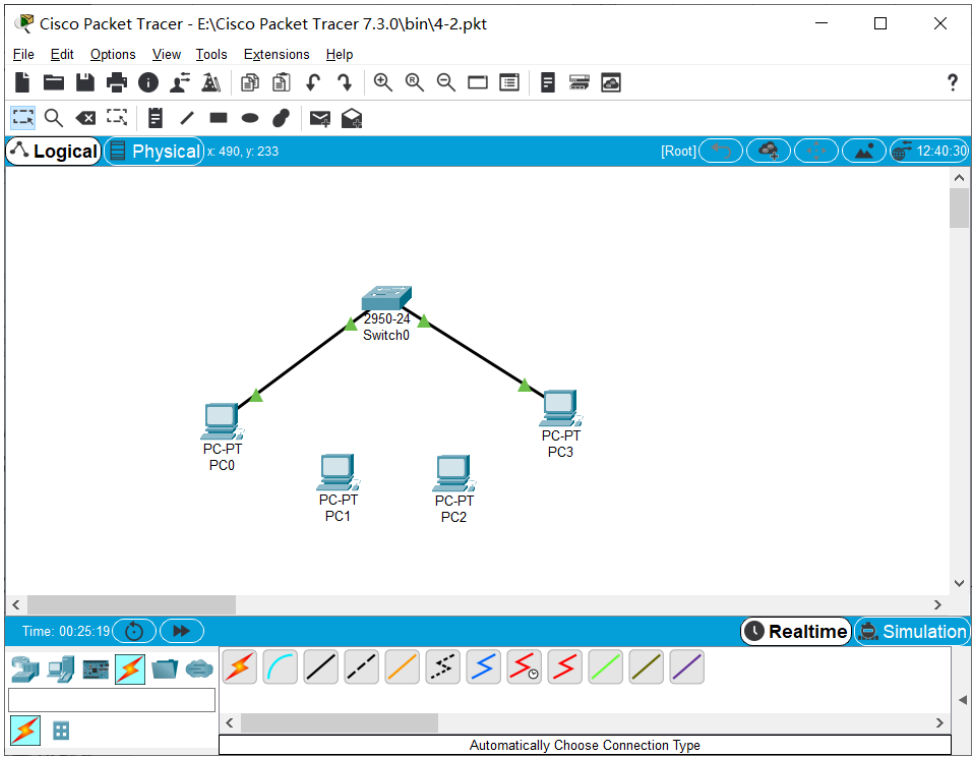
可以看到访问控制列表中已经存在 pc0 和 pc1 的 mac 地址

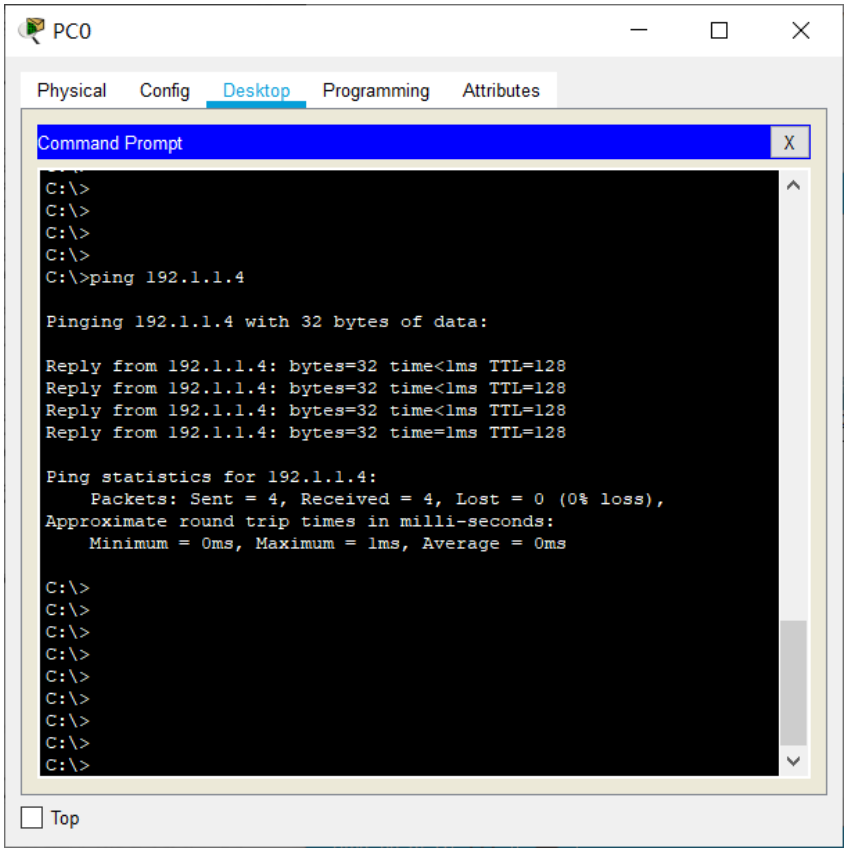
5. 删除 pc1 与交换机端口 fastethernet0/1 的连接，接入 pc2 到交换机 fastethernet0/1。可见无法交换 ICMP 报文。因为前面配置的时候把数量限制为 2（已经有 pc0，pc1 的记录了）





删除 pc2 与交换机的连接，再次接入 pc0 到 fastethernet0/1，可见仍然能正常通信





五、 实验分析总结及心得

1. **相关命令**

（1）**switchport port-security mac- address sticky** 将最先通过交换机端口学习到的 n 个 MAC 地址作为访问控制列表中的 MAC 地址。n 是访问控制列表的最大 MAC 地址数，由其他命令指定

（2）**show port-security address** 显示访问控制列表中的 MAC 地址

2. **实验心得**

通过这次实验，我对安全端口这方面的知识有了新的认识，学会了给交换机接口配置最大连接数等安全规则的基本操作，对它们的配置流程有了一个清晰的认识。

Cisco 交换机的端口安全功能允许你通过配置静态安全 MAC 地址实现仅允许固定设备连接，也允许你在一个端口上配置一个最大的安全 MAC 地址数，仅允许在此数之前识别到的设备连接在该端口上。当超过了所设置的最大安全端口数，将触发一个安全违例事件，在端口上配置的一个基于违例行为模式的违例行为将被执行。如果你在某个端口上配置的最大安全 MAC 地址数为 1，则设备上的该安全端口仅允许与固定设备连接。如果一个安全 MAC 地址在一个端口上进行了安全绑定，则这个 MAC 地址不能进入该端口加入的 VLAN 以外的任何其他端口，否则包将在硬件层被悄悄地丢弃。

我明白了做好端口安全配置，提高网络防护的重要性，提高了自己的安全意识。

实验二　防生成树欺骗攻击实验

六、　实验目的

(1)验证交换机优先级对构建的生成树的影响。

(2)验证生成树欺骗攻击过程。

(3)验证防生成树欺骗攻击原理。

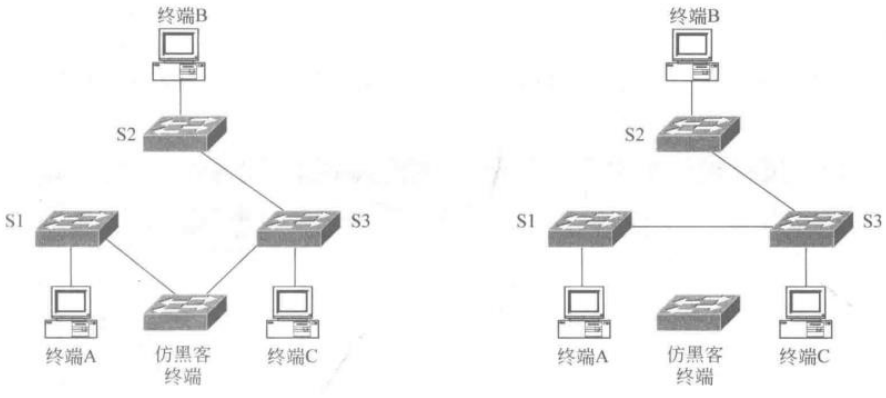
(4)验证防生成树欺骗攻击实现过程。

七、　实验原理

将仿黑客终端的交换机的优先级设置为最高后,根据如图 4.14 所示的以太网结构构建的生成树如图 4.15(a)所示,仿黑客终端的交换机成为根交换机,终端 A 与终端 B 和终端 C 之间传输的数据经过仿黑客终端的交换机。

将交换机 Sl 和 S3 连接仿黑客终端的交换机的端口设置为 BPDU 防护端口后，仿黑客终端的交换机一旦发送 BPDU,交换机 Sl 和 S3 将关闭连接仿黑客终端的交换机的端口,导致仿黑客终端的交换机不再与网络相连,仿黑客终端的交换机不再成为如图 4.15(b)所示的重新构建的生成树的一部分,终端之间传输的数据不再经过仿黑客终端的交换机。

八、　实验环境/实验拓扑图

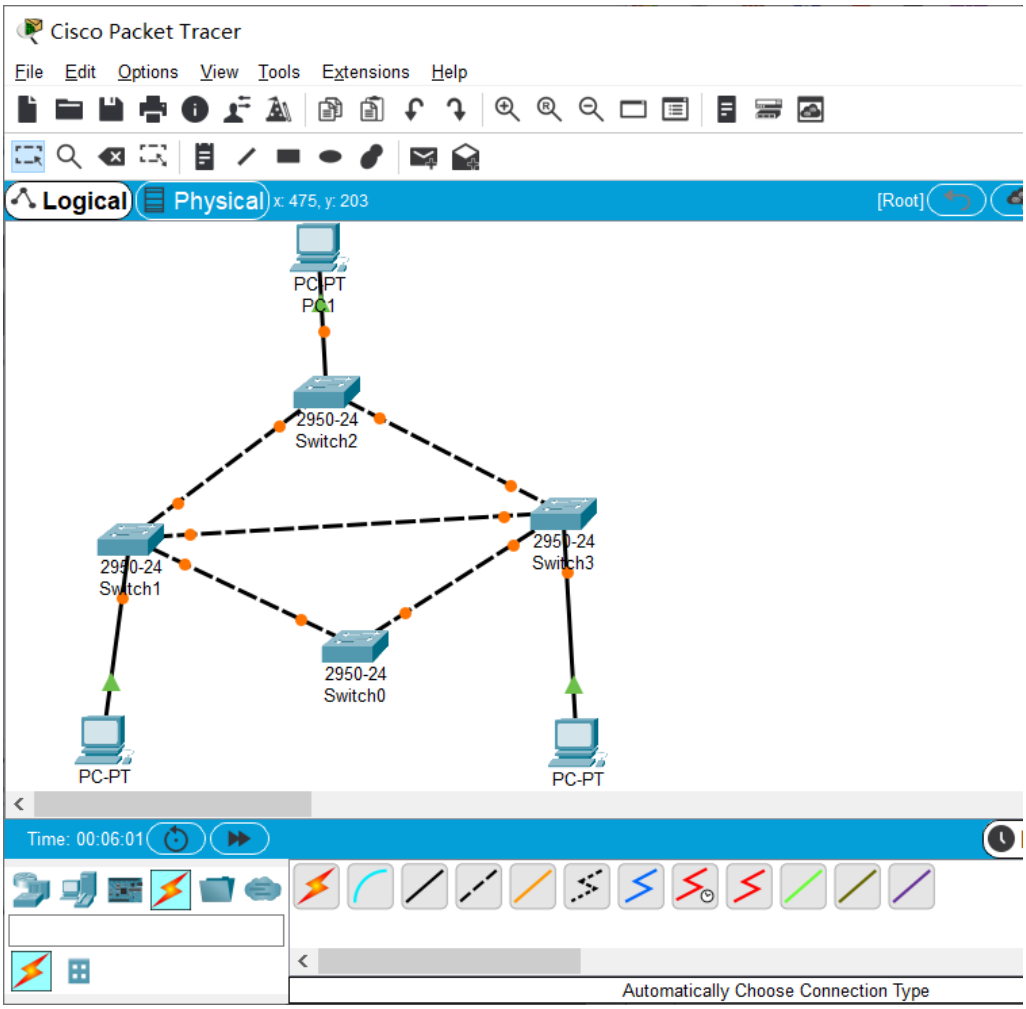


(a) 以仿黑客终端的交换机为根的生成树　　(b) 配置DBDU防护端口后的生成树

图 4.15　生成树欺骗攻击和防御过程

九、 主要操作步骤及实验结果记录

1. 完成拓扑图连接

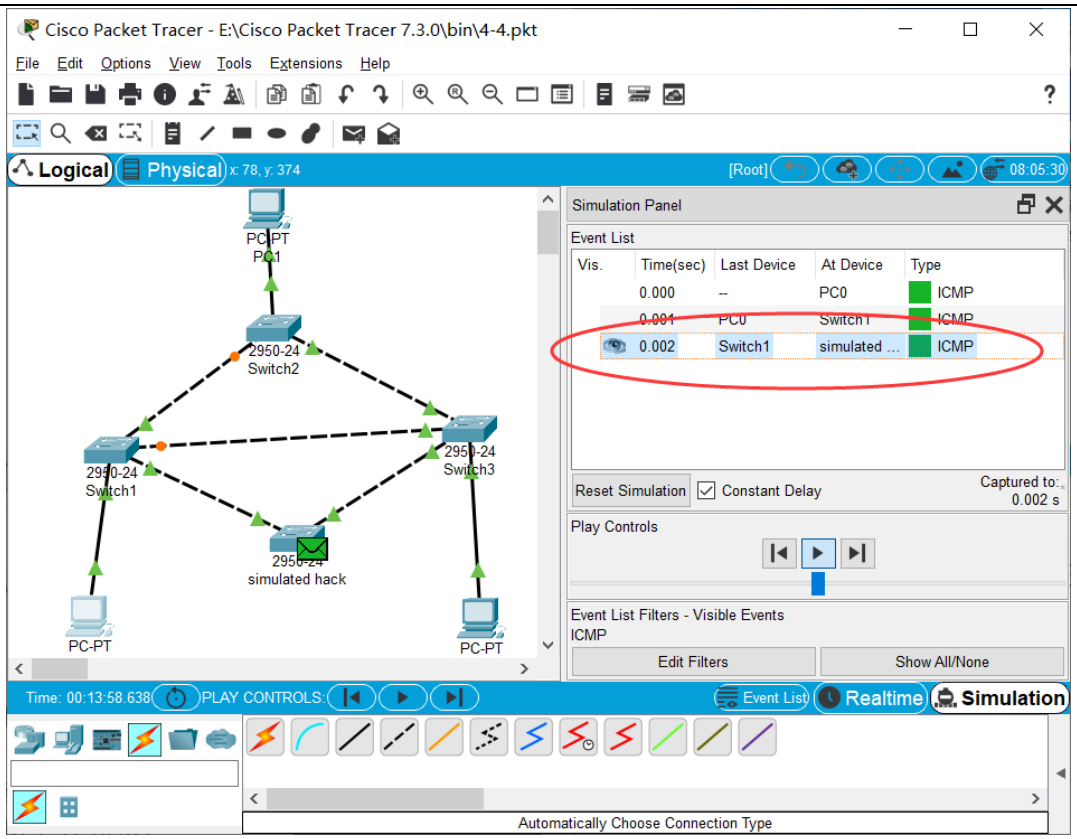


2. 完成终端网络信息的配置过程，将仿黑客终端的交换机配置成根交换机

黑客终端的交换机配置

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree mode pvst
Switch(config)#spanning-tree vlan 1 root primary
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

3. 启用模拟操作模式，用 pc0 发送 ICMP 包给 pc1，发现 ICMP 包惠经过黑客终端的交换机



4. 将交换机 switch1 和 switch3 连接黑客终端的交换机的端口（这里二者都是 fastethernet0/3）设置为 BPDU 防护端口。一旦黑客终端的交换机向 switch1 和 switch3 发送 BPDU，switch1 和 switch3 立即关闭连接黑客终端交换机的端口，对其进行隔离。

switch1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree mode pvst
Switch(config)#interface fastethernet 0/3
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on
port FastEthernet0/3 with BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/3, putting 0/3
in err-disable state

exit
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

switch3

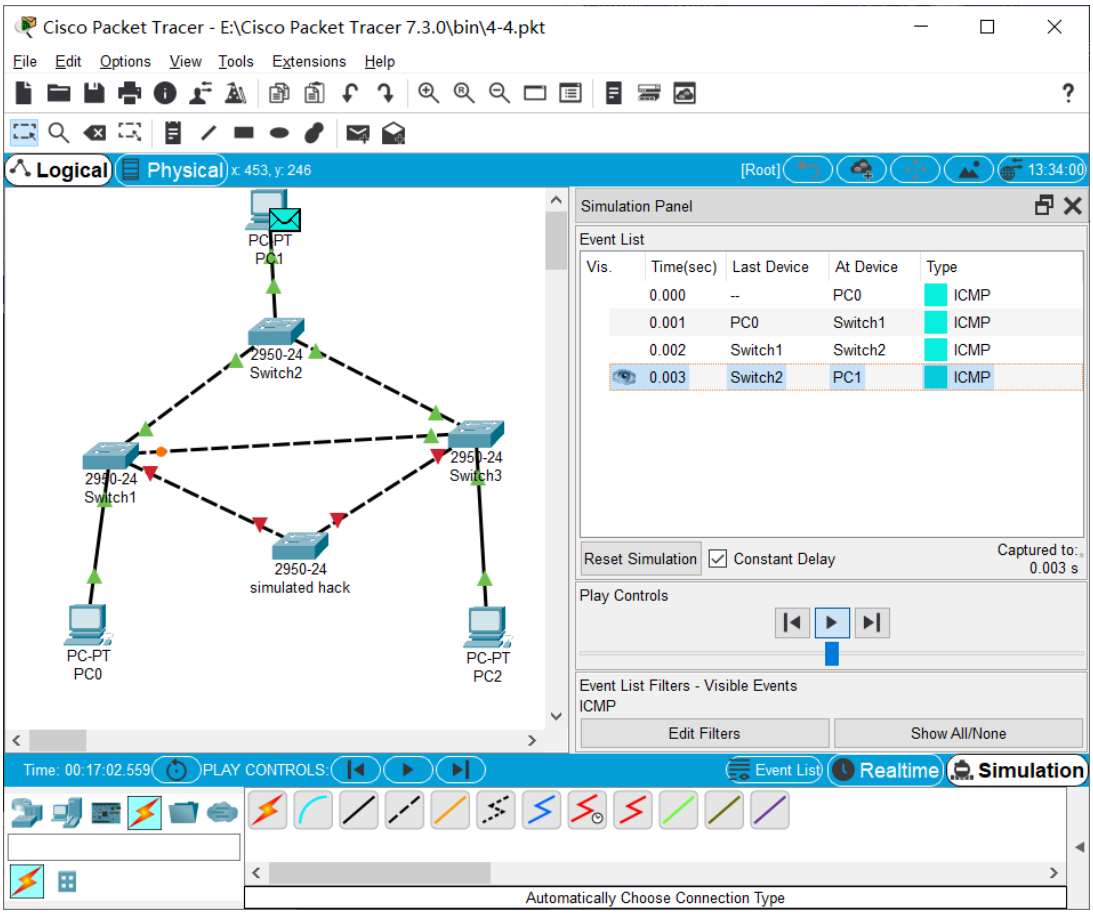
```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree mode pvst
Switch(config)#interface fastethernet 0/3
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#ex%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on
port FastEthernet0/3 with BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/3, putting 0/3
in err-disable state


%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
```

5. 切换到模拟模式，可见黑客终端的交换机不再是生成树的组成部分。使用 pc0 发送 ICMP 包给 pc1，发现数据包不再经过黑客终端的交换机进行传输。



十、 实验分析总结及心得

1. **命令列表**

（1）**spanning-tree mode { pvst rapid-pvst}**设置交换机生成树协议工作模式,可以选择的工作模式有 pvst 和 rapid-pvst

（2）**spanning-tree vlan vlan- id priority priority** 设置交换机构建基于 VLAN 的生成树时具有的优先级。参数 vlan-id 用于指定 VLAN,参数 priority 用于指定优先级

（3）**spanning-tree vlan olan-id root primary** 将交换机设置成基于 VLAN 的生成树的主根交换机。参数 vlan-id 用于指定 VLAN

（4）**spanning-tree bpduguard { disable |enable}** enable 选项用于将端口设置为 BPDU 防护端口,disable 选项用于将端口从 BPDU 防护端口还原为普通端口。某个端口设置为 BPDU 防护端口后,一旦通过该端口接收到 BPDU,交换机将立即关闭该端口

2. **实验心得**

通过这次实验，我对生成树协议这方面的知识有了新的认识，学会了防御黑客终端的交换机服务器接入生成树网络的基本操作，对黑客们的生成树欺骗攻击流程有了一个的深刻的认识。也对通过交换机构建生成树的过程有了更深入的理解，明白了做好防御生成树欺骗攻击的必要性，以及提高网络防护的重要性，提高了自己的安全意识。